RE-READING "SOUSVEILLANCE: INVENTING AND USING WEARABLE COMPUTING DEVICES FOR DATA COLLECTION IN SURVEILLANCE ENVIRONMENTS"

TED DIEHL, tdiehl@gsd.harvard.edu

SOUSVEILLANCE: INVENTING AND USING WEARABLE COMPUTING DEVICES FOR DATA COLLECTION IN SURVEILLANCE ENVIRONMENTS

Steve Mann, Jason Nolan, and Barry Wellman

Readings Bibliographical Reference in Chicago Style

1. Text Summary and Analysis

The term "sousveillance" is best understood as a play on the word "surveillance." "Surveillance" comes from the French words "sur" and "veiller," which mean, respectively, "on" and "watch." "Sousveillance" subverts this term, quite literally, by replacing the term "sur" with "sous," meaning "below." Thus "on watch" becomes "below watch."

Just as the word itself is a play on the word "surveillance," the very notion of sousveillance is a reaction to surveillance. Thus, a brief explanation of surveillance is necessary to understand the context in which sousveillance operates.

Surveillance finds its roots in Jeremy Bentham's Panopticon. Panopticism disrupted the traditional relationship between watcher and watched. Previously, the person being watched would be able to see his or her observer, and more importantly, when he or she was being watched. This granted the watched a degree of power equal to that of the watcher. The introduction of the Panopticon rendered this relationship inherently unequal. The watched no longer knows when he or she is being watched. This forces the person being watched to behave in such a manner that he or she is being watched at any moment, which indeed he or she could be. In our day, security cameras do all the watching. When there is one nearby, it may prompt people to act as if they are being watched, when in reality there might not be anyone behind the cameras at all.

Surveillance in America became rampant after September 11th. The aftermath saw a 40% increase in security cameras in New York's financial district, close to the site of Ground Zero. In the United States as a whole, there have been 30 million more security cameras installed than before 9/11. However, the most pervasive act of surveillance in America is perhaps the Patriot Act, which was passed in October of 2011, just a month after the terrorist attacks. There are many ways in which the Patriot Act violates privacy and increases surveillance in America. The following are a few of the significant allowances of this Act:

Roving Wiretaps: Allows police to obtain warrant for surveillance of unspecified persons within a certain area, and allows wiretap access to mobile cellular and satellite telephones, voicemail messaging, voice over internet, and related technology

Sneak and Peek Warrants: "Sneak and peek" warrants authorize the police to conduct surreptitious searches or wiretaps without announcing their presence or notifying the person who is the target of the investigation at the time of the search.

Imposition of Gag Orders: When a federal police search warrant is used to wiretap computers or obtain patron records from a business (i.e., public library or bookstore) the merchant or employee can be prohibited from notifying the patron suspect

Monitoring and Reporting Financial Transactions: Financial institutions are now required to report "potentially unlawful activity" on current or former bank customers or employees to the federal authorities.

Disclosure of Educational Records: Upon "certification" that the request involves a terrorism investigation, educational institutions are also required under the Patriot Act to disclose all educational records to the police, once directed by a court order.

This is the state of surveillance in America today, and it is to these conditions that sousveillance reacts. Sousveillance can best be defined as the resituation of technologies of surveillance and control on individuals, offering panoptic technologies to help them observe those in authority. Perhaps the best known example of sousveillance is the videotaping of the Rodney King beating. In this instance, a parolee was pulled over for suspected drunk driving. After resisting arrest, several police officers proceed to beat him repeatedly. Nearly the entire incident was caught on tape, and aired the next day by a major Los Angeles network. Because it was a private citizen videotaping those in authority (the police), this counts as an act of sousveillance.

In 2001, Steve Mann and several others participated in an experiment to gauge people's reactions to sousveillance and surveillance technology. They conducted a series of 5 "performances" of people wearing sousveillance devices to observe those in authority. These performances were held on busy streets and in shopping malls. This is a summary of their findings:

Performance 1: In performance one, the performer wore a wearable computer consisting of a visible camera and a projection of images on the ground. These images were either images taken by the camera (of passers-by), or of product displays. They found, through this performance, that most people were more open to product displays and advertising than to artistic and satirical displays. They were very approachable, with people often stopping to ask what the performer was selling or even to ask for directions, assuming the person was a authority on the local area.

Performance 2: Performance two was similar to performance one, in that the performer wore a wearable computer with a camera and image projection on the ground, however, in this case the camera was hidden. The live images of the camera would be used in marketing, and provocative text messages would be displayed on the ground. This performance seemed to foster more audience interaction in that people would try to find the hidden camera and they would pay more attention to an advertisement of which they were the subject. This provided an interesting blurring of the distinction between performer and spectator. Another finding of this performance is that the more surveilled a space is, the more objections were raised to their performance.

Performance 3: Performance three was like the previous performances, except that it consisted of two cameras, one motion and one still. The still camera was mounted on the performer's head, and would make an audible sound when taking a picture, alerting people to its presence. These still images were projected on the ground, along with motion picture images from the hidden camera. This performance did attract more attention from those in authority, but

because the performer seemed unable to remove the camera, the performance became more acceptable. This performance also encouraged audience interaction, as people would bring their children over to play in the projected image.

Performance 4: Performance four consisted of the performers wearing domes, such as the security camera domes that are found on ceilings which hide the direction of the camera. These domes were attached to backpacks, or necklaces, to appear like an accessory. They would also wear a display showing an image of the performer previously in the same location asking what the domes on the ceiling were for. These images were played back to the surveillance personnel. If confronted by security, the performer would simply reply that he or she was just following orders, thus demoting him/herself and rendering the performance more acceptable.

Peformance 5: Performance five was similar to performance four. People wearing increasingly larger domes would enter a store until someone would object. They discovered that the size of the dome apparently matters. Another variation of this performance consisted of the performer wearing an “Invisibility Suit” which really was a display on the front and on the back of the performer that displayed live images from a camera mounted on the other side of the performer. This allowed someone to see what was on the other side of the performer, even though it didn’t render the person “invisible.” The theatrical nature of this performance made it more acceptable, but not as acceptable as a deference to external corporate requirements.

2.Questions and Challenges

1. Does sousveillance really challenge the authority or surveillance? How?

2. Is increasing the number of cameras fighting the system or just strengthening it?

3. Does increased surveillance bother you?

3. Documentation of Responses

Sousveillance indeed has the ability to challenge the authority of surveillance, but one has to take into account different levels of authority. Typically, only lower-level employees would interrupt the performance. Often, they even demoted themselves when objecting to sousveillance, claiming that there was a managerial policy against such actions. It is unlikely that these people were affected one way or another by sousveillance, and therefore did not question the existing system of surveillance. However, it is important to remember that this article was written in 2003, and the technology both of surveillance and sousveillance are therefore outdated. It is interesting to speculate on how you would create a new paradigm of sousveillance to provide resistance against surveillance.

A member of the class cited an example of sousveillance making an impact. In August of 2011, the hacking group “Anonymous” publicized the personal information of several individuals that were users of San Francisco’s Bay Area Rapid Transit Website. This was done in response to BART shutting down cellular service in their underground train tunnels to quell a protest. Several national newspapers publicized this act of sousveillance, and BART has received severe criticism due to their actions.

In response to the second question, someone mentioned that not only cameras, but other forms of information technology may be enabling authority while operating under a “democratic” guise. For example, Google and YouTube proclaim themselves as democratic and user-oriented. However, the amount of personal information that these is available to these websites and social networks is quite alarming. Theoretically, these democratic digital spaces may actually be spaces of authoritarian control.

Another point was raised that indeed, increasing the number of surveillance cameras will probably be more enabling to authoritarian control than disabling, but one has to accept the continual progression of technology. One has to adapt and accept these changes, or fight them on different terms. For example, hacking groups, such as the aforementioned “Anonymous” are in a better position to fight technology using technology than other forms of protest. Their motto is “Fighting the system using the system.”